Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 7, No. 7, Juli 2023, hlm. 3471-3477 http://j-ptiik.ub.ac.id

Analisis Ketahanan *Routing Protocol Open Shortest Path First* (OSPF) terhadap Serangan *Route Injection*

Satria Adi Tama[1], Mahendra Data[2], Fariz Andri Bakhtiar[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]satriaa_adi@student.ub.ac.id, [2]mahendra.data@ub.ac.id, [3]fariz@ub.ac.id

Abstrak

Protokol routing *Open Shortest Path First* (OSPF) adalah salah satu protokol *routing* yang sering digunakan dalam jaringan komputer untuk mengatur pengiriman data antara perangkat jaringan. Namun, keamanan dalam OSPF menjadi hal yang sangat penting karena ada kemungkinan terjadinya serangan yang dapat mengancam integritas dan ketersediaan layanan jaringan. Penelitian ini bertujuan untuk mengkaji ketahanan OSPF terhadap serangan *route injection*. Serangan ini menggunakan kelemahan keamanan pada OSPF yang memungkinkan penyerang untuk menyuntikkan rute palsu ke dalam tabel *routing* OSPF. Rute palsu ini dapat menyebabkan pengalihan lalu lintas data ke jaringan yang tidak dapat dipercaya atau mengganggu kinerja jaringan yang sebenarnya. Metode penelitian yang digunakan melibatkan kajian pustaka untuk memahami konsep mendasar OSPF dan serangan *route injection*. Pengujian simulasi menggunakan perangkat lunak simulator jaringan GNS3, simulasi dilakukan dengan menerapkan OSPF pada struktur jaringan yang terdiri dari beberapa router dan menguji kekuatan protokol terhadap serangan *route injection* dengan berbagai skenario. Hasil penelitian menunjukkan bahwa OSPF rentan terhadap serangan penyisipan rute. Serangan ini bisa berhasil memengaruhi aliran data dalam jaringan, dengan dampak yang bisa merugikan keamanan dan ketersediaan jaringan. Namun, beberapa tindakan mitigasi bisa diterapkan untuk meningkatkan ketahanan OSPF, seperti penggunaan autentikasi yang kuat dan pemantauan terus-menerus terhadap perubahan tabel rute. Penelitian ini memberikan pemahaman yang lebih baik tentang kerentanan OSPF dalam menghadapi serangan *route injection*. Diharapkan hasil penelitian ini dapat memberikan kontribusi pada upaya meningkatkan keamanan dan kehandalan jaringan komputer yang menggunakan OSPF sebagai protokol routing.

Kata kunci: OSPF, keamanan, *route injection*

Abstract

The Open Shortest Path First (OSPF) routing protocol is a routing protocol that is often used in computer networks to regulate data transmission between network devices. However, security in OSPF is very important because there is a possibility of attacks that can threaten the integrity and availability of network services. This study aims to examine OSPF's resistance to route injection attacks. This attack uses a security weaknesses in OSPF that allows an attacker to inject fake routes into the OSPF routing table. These fake routes can cause data traffic to be redirected to untrusted networks or interfere with real network performance. The research method used involves a literature review to understand the basic concepts of OSPF and route injection attacks. Simulation testing using the GNS3 network simulator software, the simulation is carried out by applying OSPF to a network structure consisting of several routers and testing the strength of the protocol against route injection attacks with various scenarios. The results show that OSPF is vulnerable to route insertion attacks. These attacks can successfully affect the flow of data in a network, with repercussions that can be detrimental to network security and availability. However, some mitigation measures can be implemented to improve OSPF resilience, such as the use of strong authentication and continuous monitoring of route table changes. This research provides a better understanding of OSPF vulnerabilities in facing route injection attacks. It is hoped that the results of this research can contribute to efforts to improve the security and reliability of computer networks that use OSPF as a routing protocol.

Keywords*: OSPF, security, route injection*

1. PENDAHULUAN

Protokol *routing* menentukan cara router berkomunikasi satu saman lain, menyebarkan informasi yang memungkinkan untuk memilih jalur antara dua *node* di jaringan komputer. Protokol *routing link-state* merupakan jenis kelas protokol yang paling umum dipakai. Dalam protokol *routing link-state*, setiap node menyimpan topologi di seluruh jaringan, menghitung jalur dan membagikan informasi *link-state* secara berkala. Sebagai contoh dari protokol *routing* ini terdapat *Optimized Link State Routing Protocol* (OLSR), *Intermediate System to Intermiediate System* (IS-IS), serta *Open Shortest Path First* (OSPF) yang merupakan salah satu protokol *routing* yang paling sering diterapkan pada jaringan internet (Song *et al.*, 2017).

Open Shortest Path First (OSPF) merupakan sebuah protokol *routing* berjenis *Interior Gateway Protocol* (IGP) yang bekerja berdasarkan algoritma *Shortest Path First* yang dikembangkan berdasarkan algoritma *link-state* (Sabirin dan Permana, 2017). *Open Shortest Path First* (OSPF) mendistribusikan informasi router yang tergabung dalam *autonomous system* (AS) yang kemudian disebarkan dalam beberapa *link-state advertisement* (LSA) dan disimpan dalam *link-state database* (LSDB). Untuk membentuk tabel *routing* , dilakukan perhitungan *Shortest Path First* dari *link-state database* dan apabila terjadi perubahan topologi jaringan maka akan dilakukan perhitungan ulang. *Open Shortest Path First* (OSPF) juga merupakan protokol *routing* yang dapat mempelajari berbagai rute dan memilih lebih dari satu rute untuk sampai tujuan.

Namun, protokol *routing* tersebut mempunyai kelemahan sehingga dapat diserang oleh pihak tidak bertanggung jawab untuk tujuan tertentu. *Route Injection Attack* merupakan serangan yang mengeksploitasi kerentanan *routing protocol* dan memaksa menyisipkan *node* berbahaya ke dalam rute yang ada. Begitu sudah ada di rute, maka *node* berbahaya tadi akan menyuntikkan informasi yang salah dan dapat menyebabkan beban lalu lintas sehingga terjadi transmisi ulang dan perutean yang tidak efisien (De Andŕes *et al.*, 2009).

Berdasarkan masalah diatas, dilakukan penelitian tentang dampak apa yang terjadi jika *routing protocol Open Shortest Path First* (OSPF) diserang oleh *route injection* dan menganalisa apakah dampak yang ditimbulkan akan membuat lalu lintas jaringan menjadi rusak.

2. LANDASAN KEPUSTAKAAN

Penelitian pertama berjudul ”*Novel Attacks in* OSPF *Networks to Poison Routing Table”* (Song *et al.*, 2017). Paper tersebut menjelaskan tentang serangan yang dilakukan dengan cara *adjency spoofing attack* dan *single path injection attack.* Serangan ini bertujuan untuk menangkap paket *broadcast* “*hello*” yang berisi parameter jaringan seperti *Router* ID, Area ID, *HelloInterval, RouterDeadInterval, AuType* dan yang lainnya. Jika penyerang mendapatakan paket tersebut, penyerang akan mendapatkan jalur ke *database.* Kemudian dilanjutkan dengan serangan *single injection attack* untuk mengubah tabel perutean dan dapat mengarahkannya pada situs atau bahkan dapat disadap.

Penelitian kedua berjudul “*On The Prevention of Invalid Route Injection Attack*” (Li *et al.*, 2014). Paper tersebut menjelaskan bagaimana serangan *invalid route injection* bisa berdampak pada *border router* dan membuat *router* yang lain juga terkena dampak yang sama. Prinsip dasar dari serangannya adalah menambahkan *router* yang dikontrol di *stub* dengan membangun *routing protocol Open Shortest Path First* (OSPF) dengan router normal. Sementara itu mendeklarasikan pesan palsu sehingga sumber daya *router* terkuras. Menurut penelitian tersebut, *invalid route injection attack* dapat menyebabkan kerusakan parah pada jaringan. Dikarenakan kunci dari serangan ini adalah mendeklarasikan informasi dalam jumlah yang besar kedalam jaringan yang mengakibatkan pembaruan rute dalam jumlah besar dan membuat sumber daya *router* habis.

Penelitian ketiga berjudul ” *An Attack Injection Approach to Evaluate the Robustness of Ad Hoc Networks”*(De Andŕes *et al.*, 2009). Paper tersebut menjelaskan tentang pendekatan *attack injection* yang menggunakan jaringan *ad hoc* nyata sebagai platform untuk mendapatkan parameter yang dibutuhkan untuk mengevaluasi dampak serangan tersebut pada jaringan *ad hoc*. Dampak serangan yang dapat dievaluasi dengan menghitung ukuran kinerja ketika adanya serangan dan ketiadaan serangan. Menggunakan dua *network* yang berbeda yaitu jaringan nirkabel yang berfungsi sebagai *node* yang untuk bertukar informasi dan target ekperimental sedangkan yang kedua adalah jaringan kabel

yang berfungsi untuk menghubungkan semua *node* dengan *experiment controller*. *Node* bertanggung jawab untuk mengkonfigurasi *node* jaringan dan mengendalikan alur eksperimen. Serangan sederhana menargetkan serangan pada topologi yang dapat menyebabkan penolakan layanan (*denial of service).* Sedangkan serangan aktif yang lebih kompleks mencoba mengganggu rute jaringan untuk mengambil alih *target data flows* dan penurunan data paket, mengubah urutan bahkan isinya.

2.1 Routing

Routing adalah proses memindahkan data dari satu *network* ke *network* lain dengan cara meneruskan paket data melalui *gateway*. Routing menentukan data akan dikirim agar sampai tempat tujuan yang diinginkan (Moonlight dan Suhardi, 2012). Router mempelajari informasi *routing* berisi sumber jaringan dan tujuan jaringan yang ditempatkan dalam *routing table.* Router menggunakan *routing table* untuk menentukan port mana yang digunakan untuk meneruskan paket ke *destination address* mereka.

2.2 *Open Shortest Path First* (OSPF)

Open Shortest Path First merupakan routing protokol berjenis Internet Gateway Protocol (IGP) yang bekerja berdasarkan algoritma Shortest Path Fist yang dikembangkan berdasarkan algoritma link-state (Sabirin dan Permana, 2017). OSPF mendistribusikan informasi router yang tergabung dalam autonomous system (AS). Informasi status tersebut berupa prefix IP, network mask, jenis jaringan yang digunakan, dan perangkat yang terhubung dalam suatu jaringan. Informasi tersebut disebarkan dalam beberapa link-state advertisement (LSA) dan disimpan dalam link-state database (LSDB). Dari database ini perhitungan Shortest Path First dilakukan untuk membentuk routing table.

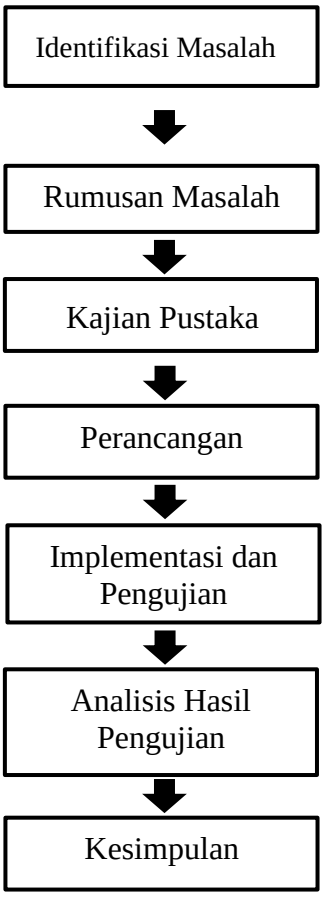
Perhitungan ulang terhadap Shortest Path First dilakukan jika terjadi perubahan pada topologi jaringan. Dengan adanya distribusi routing yang teratur maka penggunaan bandwidth lebih efisien dan lebih presisi dalam menentukan rute terbaik dalam mengirimkan paket

2.3 *Route Injection Attack*

Route Injection Attack merupakan serangan yang mengeksploitasi kerentanan *routing protocol* dan memaksa menyisipkan *node* berbahaya ke dalam rute yang ada. Begitu sudah ada di rute, maka *node* berbahaya tadi akan menyuntikkan informasi yang salah dan dapat menyebabkan beban lalu lintas sehingga terjadi transmisi ulang dan perutean yang tidak efisien (De Andŕes *et al.*, 2009). .

3. METODE PENELITIAN

Adapun tahapan-tahapan dalam membangun penelitian ini dapat disimpulkan pada diagram alur metodologi penelitian seperti pada Gambar 3.1.



Gambar 3.1 Diagram alur penelitian

Langkah pertama yang harus diambil adalah mengidentifikasi masalah untuk memperoleh informasi yang berhubungan dengan kegiatan yang sedang dilakukan. Identifikasi masalah dapat dilakukan melalui observasi atau dengan mengacu pada literatur yang ada baik berupa teks, video, suara, atau sumber lainnya. Untuk memperkaya informasi yang diperoleh, penelitian melakukan studi literatur berupa teks dan video.

Pada tahap kajian pustaka dilakukan pengumpulan referensi yang relevan dengan topik penelitian guna mendukung penulisan laporan penelitian. Referensi tertulis dan pemahaman tentang topik penelitian diperoleh dari jurnal dan sumber-sumber terkait lainnya. Beberapa topik yang terkait antara lain protokol *routing* OSPF, serangan *route injection*, *passive interface* dan *authentication* MD5..

Perancangan berupa rangkaian langkah-langkah yang akan diambil, yaitu perancangan analisis kebutuhan yang berisikan perangkat keras dan perangkat lunak yang digunakan untuk penelitian. Perancangan simulasi jaringan berisikan rancangan yang akan digunakan untuk membuat jaringan yang saling terhubung menggunakan protokol *routing* OSPF dan melakukan serangan pada jaringan tersebut. Perancangan skenario pengujian dilakukan untuk memperoleh data agar dapat dianalisis. Terdapat beberapa skenario yang dilakukan pada perancangan skenario pengujian yaitu pengujian serangan tanpa keamanan, pengujian serangan menggunakan *passive interface*, pengujian serangan menggunakan *authentication* MD5..

Setelah melakukan perancangan, langkah selanjutnya yaitu Implementasi Sistem. Suatu proses pengubahan spesifikasi sistem menjadi sistem yang dapat dieksekusi untuk melakukan pengujian berdasarkan perancangan sebelumnya. Tahapan dalam melakukan implementasi ini antara lain adalah implementasi lingkungan, konfigurasi router, melakukan serangan *route injection*, konfigurasi *passive interface* dan konfigurasi *authentication* MD5.

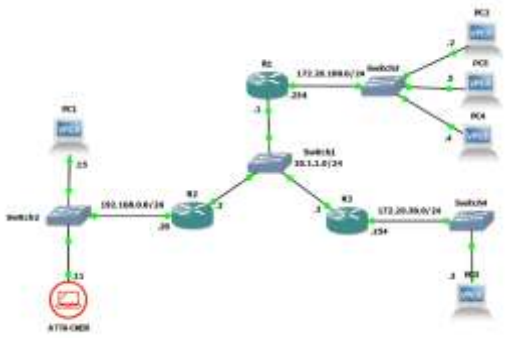
Pengujian yang dilakukan pada penelitian ini bertujuan untuk memeriksa dampak yang terjadi pada router yang diserang menggunakan serangan *route injection* pada simulator jaringan GNS3.

Langkah terakhir dalam penelitian ini adalah untuk menarik kesimpulan dari hasil pengerjaan yang telah dilakukan dan memberikan rekomendasi untuk penelitian selanjutnya yang memiliki topik serupa. Selain itu, tahap ini juga berfungsi sebagai solusi untuk rumusan masalah yang telah ditentukan

4. IMPLEMENTASI

4.1 Menjalankan Simulasi

Simulasi jaringan pada penelitian ini



Gambar 4.1 Topologi yang digunakan

menggunakan simulator jaringan GNS3 dan terlebih dahulu membuat topologi jaringan yang akan digunakan terdapat tiga router yang terhubung pada *Switch* 1, masing-masing router terhubung juga dengan *switch* menuju beberapa PC. Kemudian terdapat *attacker* yang terhubung dengan *Switch2* untuk melakukan serangan melalui router R2. Topologi terlihat seperti gambar 4.1.

Untuk menjalankan simulasi tersebut perangkat keras dan perangkat lunak yang dibutuhkan ada pada tabel 1 dan tabel 2 yang ada dibawah ini.

Tabel 1 Spesifikasi Perangkat Keras

Spesifikasi	Keterangan
Processor	Intel Core i3-3110M @ 2.40 GHz, 2400Mhz, 2 Core(s)
Memory	12288 MB
Harddisk	SSD 256 GB + 120GB

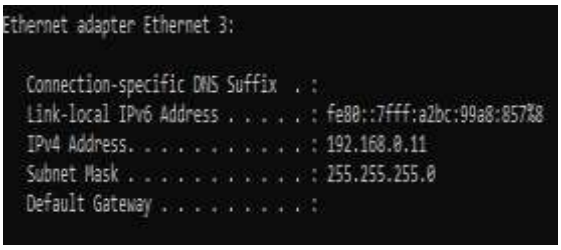
Tabel 2 Spesifikasi Perangkat Lunak

Perangkat Lunak	Deskripsi
Sistem Operasi Windows 10 64 bit	Merupakan sistem operasi yang digunakan untuk menjalankan seluruh kebutuhan perangkat lunak yang dibutuhkan dalam penelitian
Graphical Network Simulator (GNS3)	Membuat simulasi jaringan yang digunakan untuk penelitian

Loki Pentesting Tool	*Tool* yang digunakan untuk melakukan serangan ke topologi jaringan yang sudah dibuat
Wireshark	Untuk mengetahui *traffic* yang berjalan pada topologi

4.2 Serangan *Route Injection*

Pada tahap serangan *route injection*, serangan dilakukan melalui laptop yang terhubung kedalam topologi yang telah dibuat pada GNS3. Lalu, serangan dilakukan menggunakan aplikasi pentesting bernama Loki. Sebelum melakukan serangan, IP laptop diharuskan sama dengan jaringan yang akan diserang. Alamat IP yang digunakan oleh attacker adalah 192.168.0.11 seperti pada gambar 4.2 dibawah ini.



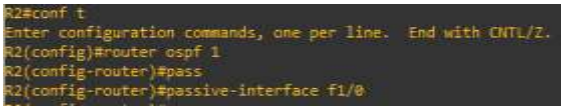
Gambar 4.2 IP *Attacker*

Setelah melakukan konfigurasi pada laptop yang bertindak sebagai *attacker*, langkah selanjutnya adalah membuka *pentesting tool* Loki. Dalam aplikasi Loki, dapat dilakukan pemindaian *interface* yang terkoneksi dengan laptop. Terlihat pada gambar 4.3 bahwa *interface* yang digunakan pada laptop menemukan IP dari router yang sudah terkoneksi.

Gambar 4.3 IP router pada Loki

4.3 Konfigurasi *Passive Interface*

Salah satu pencegahan yang dapat dilakukan untuk mencegah serangan *route injection* adalah *passive interface*. *Passive Interface* sendiri sudah tersedia pada fitur keamanan pada *routing* OSPF itu sendiri, sehingga dapat dengan mudah untuk diaktifkan. Pada tabel dibawah ini merupakan perintah dari konfigurasi *passive interface* pada router satu



Gambar 4.4 Konfigurasi *Passive Interface*

(R1).

4.5 Konfigurasi *Authentication* MD5

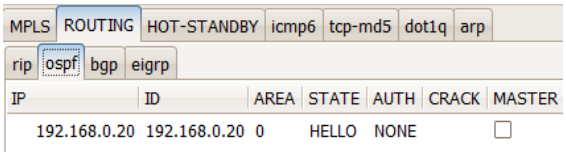
Cara selanjutnya untuk mecegah terjadinya serangan *route injection* adalah menggunakan fitur keamanan dari protokol *routing* OSPF itu sendiri yaitu *authentication.* Berikut merupakan konfigurasi pada Router 1 (R1)

Gambar 4.4 Konfigurasi *authentication* MD5

5. PENGUJIAN DAN HASIL

5.1 Pengujian Sistem

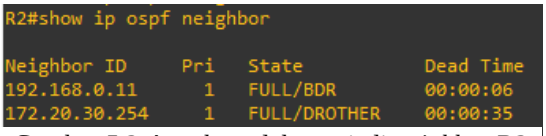
Pengujian pertama yaitu melakukan serangan *route injection* tanpa adanya fitur keamanan yang terkonfigurasi pada router. Serangan dilakukan menggunakan *pentesting tool* bernama Loki. Ketika *attacker* melakukan pemindaian, maka akan terlihat alamat IP 192.168.0.20 yang merupakan IP router yang sudah terkonfigurasi OSPF seperti yang terlihat pada gambar 5.1 dibawah ini.



Gambar 5.1 IP Router terdeteksi pada Loki

Setelah IP terdeteksi *attacker* dapat mengirimkan paket *"Hello"* agar dapat menjadi *neighbor*. Pada gambar 5.2 dibawah ini terlihat, IP *attacker* yaitu 192.168.0.11 sudah menjadi *neighbor* pada router.

Selanjutnya *attacker* melakukan *route injection* ke *network* 172.20.100.0 untuk



Gambar 5.2 *Attacker* telah menjadi *neighbor* R2

membelokkan jalur sehingga paket yang dikirimkan melalui *network* 172.20.100.0 akan melewati *attacker* sebelum sampai pada penerima.

Serangan kedua yaitu melakukan serangan dengan terkonfigurasinya *passive interface*. Perintah untuk mengkonfigurasi *passive interface* cukup mudah seperti gambar 5.3 di bawah ini. *Passive interface* membuat *interface* tidak terlihat dikarenakan tidak mengirimkan paket *"Hello"* sehingga tidak dapat bertukar informasi pada router yang terhubung. Hal itu membuat IP router tidak terdeteksi juga pada aplikasi Loki sehingga *attacker* tidak dapat melakukan serangan pada router.

Serangan berikutnya yaitu melakukan serangan dengan terkonfigurasinya

```
R2(config)#router ospf 1
R2(config-router)#passive inter
R2(config-router)#passive-inter
R2(config-router)#passive-interface f1/1
#ip ospf message-digest-key 1 md5 secret123
#ip ospf
#ip ospf authen
#ip ospf authenticationmess
#ip ospf authentication mess
#ip ospf authentication message-digest
```

Gambar 5.4 Konfigurasi *authentication* MD5

authentication MD5. Perintah untuk mengkonfigurasi *authentication* MD5 seperti gambar 5.4 dibawah ini dan dapat menggunakan kata sandi sesuai dengan keinginan seperti contoh yaitu "secret123". *Authentication* MD5

membuat *attacker* tidak bisa langsung untuk

Gambar 5.5 Tampilan pada aplikasi Loki

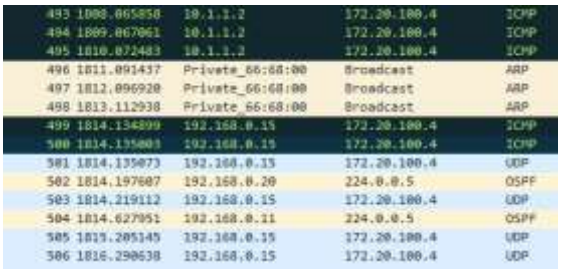
menyerang dengan mengirimkan paket *"Hello"* dikarenakan *interface* router yang dituju terenkripsi. Pada aplikasi Loki pada gambar 5.5 terlihat bahwa IP 192.168.0.20 pada kolom AUTH tertulis CRYPT yang artinya terenkripsi.

5.2 Hasil Pengujian

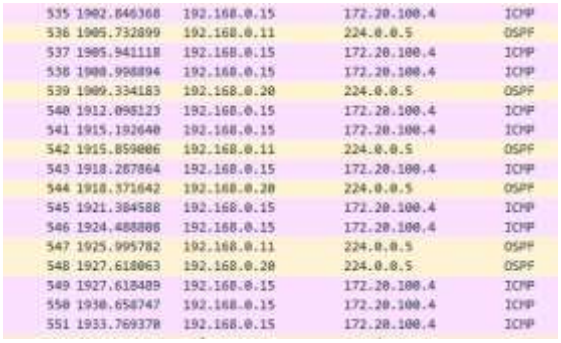
Hasil dari serangan tanpa terkonfigurasi keamanan apapun adalah *attacker* dapat melihat paket yang dikirim dari PC4 ke PC2 sebagai penerima terlihat pada *capture traffic* pada wireshark pada gambar 5.6 dan 5.7 dimana PC4 mengirimkan protokol UDP dan ICMP.

Jika *attacker* dapat mengetahui paket yang dikirimkan oleh PC pengirim maka akan sangat berbahaya jika paket atau data tersebut bersifat penting.

Hasil dari serangan selanjutnya yaitu serangan yang sudah terkonfigurasi *passive interface*. *Passive interface* membuat router

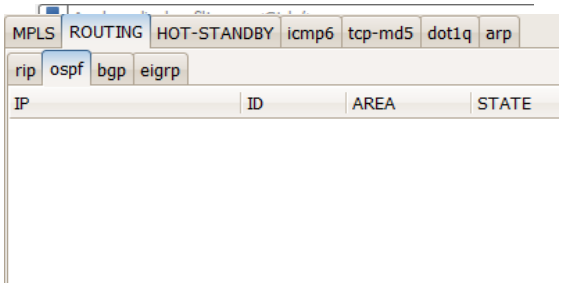


Gambar 5.6 *Capture traffic* pada wireshark

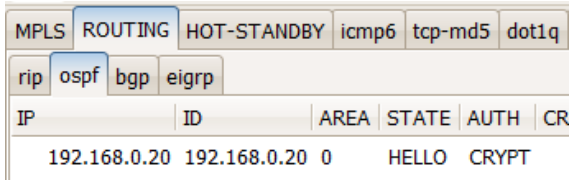


Gambar 5.7 *Capture traffic* PING dari PC4

tidak mengirimkan paket *"Hello"* yang membuat router lain tidak bisa melakukan pertukaran informasi yang dapat berubah menjadi *neighbor* router tersebut. Pada aplikasi Loki terlihat jika tidak terdeteksi IP dari router R2 begitu juga pada wireshark juga tidak menemukan *traffic* pada router tersebut seperti pada gambar 5.8 dan gambar 5.9.



Serangan selanjutnya yaitu serangan kepada router yang sudah terkonfigurasi *authentication* MD5. Ketika *attacker* mencoba menyerang



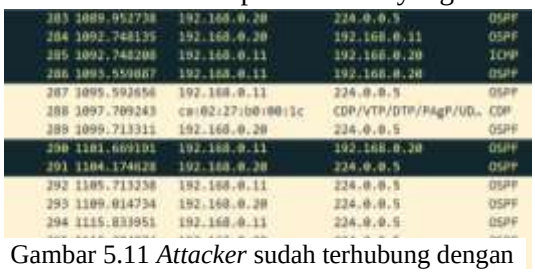
Gambar 5.10 Loki mendeteksi jika IP terenkripsi

Gambar 5.9 Loki tidak mendeteksi IP router

router tersebut, yang terjadi adalah tidak bisa langsung mengirimkan paket *"Hello"* agar dapat bertukar informasi dan menjadi *neighbor* R2 seperti pada gambar 5.10. Jika seperti maka *attacker* tidak bisa menyerang router tersebut. Namun, *authentication* MD5 ini masih bisa untuk di *cracking* oleh *attacker*. Dengan menu yang ada pada Loki untuk *cracking*, *attacker* harus menebak kata sandi yang memungkinkan untuk membuka enkripsi tersebut. Jika *attacker* berhasil melakukan *cracking*, maka *attacker* bisa langsung terhubung dan melakukan serangan pada router R2 seperti yang terlihat pada gambar 5.11.

6. KESIMPULAN

Berdasarkan penelitian yang sudah



Gambar 5.11 *Attacker* sudah terhubung dengan R2

dilakukan, dampak dari serangan *route injection* terhadap *routing procotol* OSPF adalah paket yang dikirimkan oleh PC pengirim akan diketahui oleh *attacker*. Jika paket tersebut merupakan hal yang pentin maka akan sangat berbahaya jika *attacker* dapat mengetahui paket tersbut.

Celah keamanan yang ada di *routing protocol* OSPF adalah terletak pada *interface* router yang tidak diberi fitur keamanan apapun sehingga dapat dengan mudah untuk disusupi. Meskipun masih bisa menggunakan *authentication* MD5 untuk melakukan pencegahan agar tidak disusupi alamat palsu, *attacker* masih memungkinkan untuk menebak atau mencoba memecahkan kata sandi yang telah dibuat. Jika *attacker* berhasil, maka akan dengan mudah untuk disusupi alamat palsu dari *attacker*.

Dalam *routing protocol* OSPF ternyata mempunyai fitur pengamanan yang belum terkonfigurasi karena secara *default* tidak terkonfigurasi pengamanan apapun. Untuk mencegah serangan *route injection* pada OSPF adalah dengan mengaktifkan fitur pengamanan *passive interface* pada *interface router* yang mengarah pada *end device*. Kemudian mengaktifkan autentikasi MD5 agar ketika *attacker* akan menyusupi *interface* router, dapat terhambat dengan kunci yang sudah dikonfigurasi dengan kata kunci yang sudah dibuat dengan baik

7. DAFTAR PUSTAKA

Song, Y. *et al.* (2017) "Novel attacks in OSPF networks to poison routing table," *IEEE International Conference on Communications* [Preprint]. Tersedia pada: https://doi.org/10.1109/ICC.2017.7996829.

Sabirin, F. dan Permana, R. (2017) "Perbedaan Routing Menggunakan Routing Information Protocol (RIP) Dengan Open Shortest Path First (OSPF)," *Cybernetics*, 1(02), hal. 120. Tersedia pada: https://doi.org/10.29406/cbn.v1i02.748.

Li, M. *et al.* (2014) "On the prevention of invalid route injection attack," *IFIP Advances in Information and Communication Technology*, 432(February 2008), hal. 294–302. Tersedia pada: https://doi.org/10.1007/978-3-662-44980-6_33.

Moonlight, L.S. dan Suhardi, S. (2012) "Pengaruh Model Jaringan Terhadap Optimasi Routing Open Shortest Path First (Ospf)," *Teknologi*, 1(2), hal. 68–80. Tersedia pada: https://doi.org/10.26594/teknologi.v1i2.56.

De Andŕes, D. *et al.* (2009) "An attack injection approach to evaluate the robustness of ad hoc networks," *2009 15th IEEE Pacific Rim International Symposium on Dependable Computing, PRDC 2009*, hal. 228–233. Tersedia pada: https://doi.org/10.1109/PRDC.2009.43.